Съвет на
Европейския съюз

Брюксел, 19 ноември 2018 г.
(OR. en)

14413/18

CYBER 285
CSDP/PSDC 669
COPS 444
POLMIL 214
EUMC 193
RELEX 978
JAI 1154
TELECOM 415
CSC 328
CIS 13
COSI 290

РЕЗУЛТАТИ ОТ РАБОТАТА

От:	Генералния секретариат на Съвета
Дата:	19 ноември 2018 г.
До:	Делегациите
Относно:	Политическа рамка на ЕС за кибернетична отбрана (актуализация 2018 г.)

Приложено се изпраща на делегациите политическата рамка на ЕС за кибернетична отбрана (актуализация 2018 г.), приета от Съвета на 3652-рото му заседание, проведено на 19 ноември 2018 г.

ПРИЛОЖЕНИЕ

ПОЛИТИЧЕСКА РАМКА НА ЕС ЗА КИБЕРНЕТИЧНА ОТБРАНА

(АКТУАЛИЗИРАНА ПРЕЗ 2018 Г.)

Обхват и цели

В отговор на променящите се предизвикателства, свързани със сигурността, ЕС и неговите държави членки трябва да укрепят устойчивостта на киберпространството и да развиват стабилни способности в областта на кибернетичните сигурност и отбрана.

Политическата рамка на ЕС за кибернетична отбрана (ПРКО) подкрепя развитието на способности за кибернетична отбрана на държавите — членки на ЕС, както и укрепването на кибернетичната защита на инфраструктурата на ЕС, свързана със сигурността и отбраната, без да се засяга националното законодателство на държавите членки и законодателството на ЕС, включително обхвата на кибернетичната отбрана, когато е определен такъв.

Киберпространството е петата област на операции, наред с областите суша, вода, въздух и космическо пространство: успешното изпълнение на мисиите и операциите на ЕС става все по-зависимо от непрекъснатия достъп до сигурно киберпространство, за което се изискват стабилни и устойчиви оперативни способности в областта на киберпространството.

Целта на актуализираната ПРКО е да се развие по-нататък политиката на ЕС за кибернетична отбрана, като се вземат предвид съответните постижения в други имащи отношение форуми и области на политиката и прилагането на ПРКО от 2014 г. насам. В ПРКО са определени приоритетните области за кибернетична отбрана и е пояснена ролята на различните европейски участници, като същевременно се зачитат в пълна степен отговорностите и компетентностите на участниците от Съюза и на държавите членки, както и институционалната рамка на ЕС и неговата автономност при вземане на решения.

Контекст

В заключенията на Европейския съвет относно ОПСО от декември 2013 г., както и в заключенията на Съвета относно ОПСО от ноември 2013 г. бе отправен призив за разработването на политическа рамка на ЕС за кибернетична отбрана въз основа на предложение на върховния представител, в сътрудничество с Европейската комисия и Европейската агенция по отбрана (EDA). Политическата рамка на ЕС за кибернетична отбрана беше приета от Съвета на 18 ноември 2014 г.[1] и нейното прилагане от този момент нататък доведе до конкретни резултати, които допринесоха за значително укрепване на способностите на държавите членки за кибернетична отбрана. Като част от годишния си доклад за 2017 г. за прилагането на политическата рамка за кибернетична отбрана[2] и като вземат предвид инициативите на ЕС в областта на сигурността и отбраната, по-конкретно координирания годишен преглед на отбраната (КГПО), постоянното структурирано сътрудничество (ПСС), Европейския фонд за отбрана (ЕФО) и Пакта за гражданските мисии по линия на ОПСО, както и преразглеждането през 2018 г. на плана за развитие на способностите (ПРС) и плана за развитие на гражданските способности (ПРГС), държавите членки призоваха за актуализиране на политическата рамка на ЕС за кибернетична отбрана.

Кибернетичната сигурност е приоритет в рамките на глобалната стратегия за външната политика и политика на сигурност на ЕС и в рамките на равнището на амбиция на ЕС[3]. В глобалната стратегия се набляга на необходимостта от увеличаване на способностите за защита на ЕС и неговите граждани и за реагиране на външни кризи. В глобалната стратегия се подчертава нуждата от укрепване на ролята на ЕС като общност на сигурността. В този контекст, усилията в областта на сигурността и отбраната следва да засилят и стратегическата роля на ЕС и способността му да действа самостоятелно, където и когато е необходимо, и при възможност съвместно с партньори. Тези цели изискват повече сътрудничество в областта на развитието на способностите, насърчаване на ефективността и оперативната съвместимост на постигнатите по този начин граждански и военни способности.

---

1 Док. 15585/14 на Съвета, 18.11.2014 г.
2 Док. 15870/17 на Съвета, 19.12.2017 г.
3 Заключения на Съвета относно изпълнението на Глобалната стратегия на ЕС в областта на сигурността и отбраната, 14.11.2016 г.

Общият набор предложения за прилагането на съвместната декларация, подписана от председателя на Европейския съвет, председателя на Европейската комисия и генералния секретар на Организацията на Северноатлантическия договор във Варшава на 8 юли 2016 г.[4], включва конкретни действия за разширяване на сътрудничеството между ЕС и НАТО в областта на кибернетичните сигурност и отбрана, включително в контекста на мисиите и операциите, както и по отношение на развиването на способности за кибернетична отбрана, изследвания и технологии, обучение, образование, учения и интегриране на киберсигурността в управлението на кризи. Това сътрудничество се осъществява при пълно зачитане на принципите на откритост, прозрачност, приобщаване, реципрочност и автономност на ЕС при вземането на решения. Техническото споразумение между екипа на ЕС за незабавно реагиране при компютърни инциденти (CERT-EU) и екипа на НАТО за реагиране при компютърни инциденти (NCIRC), подписано през февруари 2016 г., улеснява обмена на техническа информация с цел по-доброто предотвратяване, откриване и реагиране на киберинциденти в рамките на двете организации.

Следва да се припомни, че няколко политики на ЕС допринасят за постигане на целите на политиката в областта на кибернетичната отбрана, изложени в настоящия документ, като в тази рамка са взети под внимание и съответните разпоредби и политическа и технологична помощ в гражданската област. През юли 2016 г., например, Европейският парламент и Съветът приеха Директивата за мрежова и информационна сигурност[5], с което ще се повиши цялостната готовност на държавите членки за борба с кибернетични заплахи, и ще се засили сътрудничеството в целия ЕС. С настоящата директива се установяват мерки с цел постигане на високо общо ниво на сигурност на мрежите и информационните системи в Съюза, така че да се подобри функционирането на вътрешния пазар. Крайният срок за транспониране на директивата е 9 май 2018 г.

---

[4] Заключения на Съвета относно прилагането на Съвместната декларация на председателя на Европейския съвет, председателя на Европейската комисия и генералния секретар на Организацията на Северноатлантическия договор (6 декември 2016 г., 15283/16; 5 декември 2017 г., 14802/17)

[5] Директива (ЕС) 2016/1148 на Европейския парламент и на Съвета от 6 юли 2016 г. относно мерки за високо общо ниво на сигурност на мрежите и информационните системи в Съюза, ОВ L 194, 19.7.2016 г., стр. 1.

Предложението от септември 2017 г. за Акт за киберсигурността на ЕС включва новия мандат за Агенцията на Европейския съюз за мрежова и информационна сигурност (ENISA) и създаването на обща за целия ЕС рамка за сертифициране. След въвеждането си рамката за сертифициране следва да поддържа високи стандарти за ИКТ процеси, продукти и услуги, да бъде източник на конкурентно предимство и да повиши доверието на потребителите и възложителите на обществени поръчки. Освен това през септември 2017 г. Комисията предприе и друга стъпка, за да подготви ЕС за случаи на мащабни трансгранични киберинциденти („Blue Print“), а в момента работи съвместно с държавите членки и с други институции, агенции и органи за изготвянето на европейска рамка за сътрудничество при кризи в областта на киберсигурността, която да включва практическото операционализиране и документиране на всички съответни участници, процеси и процедури в контекста на вече съществуващите в ЕС механизми за управление на кризи и бедствия, по-специално договореностите за интегрирана реакция на ЕС при политическа криза.

Заключенията на Съвета от ноември 2016 г. относно укрепването на отбранителната способност на Европа срещу кибератаки очертават общата цел за принос към стратегическата автономност на ЕС, както е посочено в заключенията на Съвета от ноември 2016 г. относно Глобалната стратегия за външната политика и политиката на сигурност на Европейския съюз, включително в киберпространството. Европейският съвет потвърди това съобщение през юни 2018 г., като също подчерта необходимостта от укрепване на способностите за борба със заплахите за киберсигурността с произход извън ЕС.

През 2017 г. Съветът прие рамка за съвместен дипломатически отговор на ЕС срещу злонамерени действия в киберпространството („инструментариум за кибердипломация“)[6]. Очаква се рамката да насърчава сътрудничеството, да улеснява ограничаването на заплахите и да оказва влияние върху поведението на потенциалните извършители в дългосрочен план. Рамката използва мерките в областта на ОВППС, включително ограничителни мерки, с цел предотвратяване и реагиране на злонамерени действия в киберпространството. Извършителите на злонамерени дейности в киберпространството трябва да бъдат подвеждани под отговорност за своите действия, а държавите — членки на ЕС, се насърчават да продължат да развиват способността си да реагират на злонамерени дейности в киберпространството по координиран начин и в съответствие с инструментариума за кибердипломация. Държавите не следва да провеждат или подкрепят съзнателно дейности в областта на информационните и комуникационните технологии в разрез със своите задължения съгласно международното право, също така не следва съзнателно да позволяват територията им да бъде използвана за международно неправомерни деяния, при които се използват информационни и комуникационни технологии.

Съвместно съобщение[7] относно киберсигурността беше представено от Комисията и ВП/ЗП през септември 2017 г. с цел смекчаване на рисковете, произтичащи от новите заплахи. В него кибернетичната отбрана се посочва като една от основните области на действие, а ПРКО е един от стълбовете на конкретното ѝ прилагане[8].

В заключенията на Съвета от ноември 2017 г. относно кибернетичното пространство бяха отчетени увеличаващите се връзки между киберсигурността и отбраната и беше отправен призив за засилване на сътрудничеството в областта на кибернетичната отбрана, включително чрез насърчаване на сътрудничеството между гражданските и военните общности за реагиране при инциденти. Освен това в тях се изтъква, че един особено сериозен киберинцидент или криза би могъл да съставлява достатъчно основание за това държава членка да задейства клаузата на ЕС за солидарност и/или клаузата за взаимна помощ.

---

6 Заключения на Съвета относно рамка за съвместен дипломатически отговор на ЕС срещу злонамерени действия в киберпространството („инструментариум за кибердипломация“), 9916/17, 7 юни 2017 г.

7 Съвместно съобщение до Европейския парламент и Съвета: „Устойчивост, възпиране и отбрана: изграждане на силна киберсигурност за ЕС“ (13 септември 2017 г., JOIN(2017) 450 final)

8 Заключения на Съвета относно Съвместното съобщение до Европейския парламент и Съвета: „Устойчивост, възпиране и отбрана: изграждане на силна киберсигурност за ЕС“ (20 ноември 2017 г., 14435/17)

На 11 декември 2017 г. беше създадено постоянното структурирано сътрудничество (ПСС). Тази амбициозна, обвързваща и приобщаваща рамка за сътрудничество беше установена между 25 държави членки и включва ангажимент за засилване на усилията за сътрудничество в областта на кибернетичната отбрана, както и свързаните с това проекти по линия на ПСС. Първият набор от проекти по линия на ПСС, определени от участващите в ПСС държави членки през 2017 г., включва два проекта, свързани с кибернетичната отбрана: „екипи за бързо реагиране при кибератаки и екипи за взаимопомощ в областта на киберсигурността“ и „платформа за обмен на информация относно киберзаплахи и реагиране при инциденти“. Предвиждат се допълнителни групи проекти по линия на ПСС. ПСС ще развива способности за кибернетична отбрана, така че да се засили сътрудничеството между участващите държави членки и да се повиши оперативната съвместимост.

В актуализирания план за развитие на способностите на ЕС (ПРС), одобрен от Управителния съвет на EDA през юни 2018 г., кибернетичната отбрана е определена за ключов елемент, като се отчита нуждата от отбранителни кибероперации във всякакъв оперативен контекст, въз основа на усъвършенствана текуща и прогнозна ситуационна осведоменост по отношение на киберпространството, включително възможността за комбиниране на големи количества данни и разузнавателни сведения от множество източници в подкрепа на бързото вземане на решения и все по-висока степен на автоматизиране на процесите на събиране на данни, анализ и подпомагане на решенията. В ПРС 2018 по отношение на способностите за кибернетична отбрана са определени следните приоритети: сътрудничество и полезно взаимодействие със съответни участници в областта на кибернетичната отбрана и киберсигурността; научноизследователски и технологични действия в областта на кибернетичната отбрана; рамки за системен инженеринг за операциите в кибернетичното пространство; образование, обучение, учения и оценка (ETEE); отговор на предизвикателствата в областта на кибернетичната отбрана — въздушни, космически, морски и сухопътни.

И накрая, през последните няколко години се откроi ясно необходимостта от предотвратяване на конфликти, сътрудничество и стабилизиране на киберпространството от страна на международната общност. В тясно сътрудничество с други международни организации, а именно ООН, ОССЕ и Регионалния форум на АСЕАН, ЕС работи за прилагането на стратегическа рамка за предотвратяване на конфликти, сътрудничество и стабилност в киберпространството, която включва: i) прилагане в киберпространството на международното право, по-специално Устава на ООН в неговата цялост; ii) зачитане на всеобщите незадължителни норми, правила и принципи за отговорно поведение от страна на държавите; iii) разработване и прилагане на регионални мерки за изграждане на доверие. Политическата рамка за кибернетична отбрана следва също да подкрепя тези усилия.

Приоритети

В актуализираната ПРКО са определени шест приоритетни области . Основен акцент в тази политическа рамка е разработването на способности за кибернетична отбрана, както и защитата на комуникационните и информационните мрежи на ОПСО на ЕС. Други приоритетни области са: обучение и учения, научни изследвания и технологии, гражданско-военно сътрудничество и международно сътрудничество. В областта на обучението акцентът е поставен върху активизиране от страна на държавите членки на обучението в областта на кибернетичната отбрана и на обучение на командната верига на ОПСО по отношение на кибернетичната осведоменост. Освен това е важно измерението, свързано с кибернетичното пространство, да намери подходящо място в ученията, така че да се повиши способността на ЕС за реагиране на кибернетични и хибридни кризи, като се подобрят процедурите за вземане на решения и наличността на информация. Киберпространството е бързо развиваща се област и трябва да се подкрепят новите технологични постижения, както в гражданската, така и във военната сфера. Гражданско-военното сътрудничество в сферата на киберпространството е от ключово значение, за да се гарантира системен отговор на киберзаплахите. Накрая, но не на последно място, задълбочаването на сътрудничеството с международни партньори би могло да спомогне за повишаване на киберсигурността в рамките на ЕС и извън него, както и за утвърждаване на принципите и ценностите на ЕС.

В рамката са набелязани предложения и възможности за координация между съответните институции, органи и агенции на ЕС. Отразена е и важната роля на частния сектор за разработването на технологии за киберсигурността и кибернетичната отбрана.

В допълнение на това ПРКО подпомага интегрирането на елементи на кибернетичната отбрана в рамките на механизмите на Съюза за управление на кризи, когато за справянето с последиците от кибернетична криза може да са приложими определени имащи отношение разпоредби от Договора за ЕС и Договора за функционирането на ЕС[9].

1. Подкрепа за развитието на способностите на държавите членки за кибернетична отбрана

Разработването на способности и технологии за кибернетична отбрана следва да обхваща всички аспекти на изграждането на способности, в това число доктрина, ръководство, организация, личен състав, обучение, промишленост, технологии, инфраструктура, логистика и оперативна съвместимост. За тази цел държавите членки следва да увеличат усилията си за постигането на реална способност за кибернетична отбрана. ЕСВД, Комисията и EDA следва да работят заедно и да подкрепят тези усилия.

Необходима е постоянна оценка на слабите места на информационните инфраструктури, поддържащи мисиите и операциите по линия на ОПСО, както и разбиране в почти реално време за ефективността на защитата. От оперативна гледна точка, една от основните области, върху която са съсредоточени дейностите за кибернетична отбрана, ще продължи да бъде наличността, целостта и поверителността на комуникационните и информационните мрежи на ОПСО, освен ако в мандата на операциите или мисиите не е уточнено друго. Освен това, ЕСВД, в сътрудничество с държавите членки, ще продължи да интегрира киберспособности в мисиите и операциите по линия на ОПСО.

Извършителите на злонамерени дейности в киберпространството трябва да бъдат подвеждани под отговорност за своите действия. Важно е държавите — членки на ЕС, с подкрепата на ЕСВД, да насърчават взаимното сътрудничество при реагиране на злонамерени дейности в киберпространството. Инструментариумът за кибердипломация е разработен, за да се подпомогне постигането на такива взаимни действия за реагиране. ЕСВД и EDA ще организират въз основа на инструментариума за кибердипломация редовни учения, в които държавите — членки на ЕС, могат да практикуват това.

[9] Член 222 от ДФЕС и член 42, параграф 7 от ДЕС, при надлежно отчитане на член 17 от ДЕС

Предвид факта, че в националното законодателство на държавите членки и в законодателството на ЕС обхватът на кибернетичната отбрана е широк и разнообразен, ако и когато такъв е определен, е необходимо да се разработи общо и обобщено разбиране относно обхвата на кибернетичната отбрана.

Като се има предвид, че военните операции по линия на ОПСО разчитат на инфраструктура за командване, контрол, комуникации и компютри (C4), предоставяна от държавите членки, при планирането на изискванията за кибернетичната сигурност на информационната инфраструктура е необходима определена степен на стратегическо сближаване.

Като доразвиват работата на проектния екип за кибернетична отбрана към EDA с цел разработване на способности за кибернетична отбрана, EDA и държавите членки:

- ще използват ПРС и други инструменти, например КГПО, които улесняват и подпомагат сътрудничеството между държавите членки, така че да се повиши степента на сближаване в планирането на изискванията за кибернетична отбрана на държавите членки на стратегическо ниво, по-специално по отношение на наблюдението, ситуационната осведоменост, превенцията, откриването и защитата, обмена на информация, криминалистиката и способността за анализ на зловреден софтуер, извлечените поуки, овладяването на щетите, способностите за динамично възстановяване, съхраняването на разпространени данни и архивирането на данни.
- ще окажат подкрепа за текущи и бъдещи проекти за обединяване и споделяне на способности в областта на кибернетичната отбрана при военни операции (например в криминалистиката, развиването на оперативна съвместимост, определянето на стандарти).
- ще разработят, въз основа на наличния в целия ЕС опит, стандартен набор от цели и изисквания за определяне на минималното ниво на кибернетична сигурност и доверие, което държавите членки да постигнат.

ЕСВД и EDA:

- ще улеснят обмена между държавите членки в областта на националните доктрини за кибернетична отбрана, както и по отношение на програмите за наемане, задържане и изграждане на запасен корпус в областта на кибернетичната отбрана.

EDA:

- ще проучи различния обхват на свързаните с кибернетичната отбрана военни изисквания в националното законодателство и добрите практики на държавите членки. Основната цел на проучването ще бъде да се разработи корпоративна архитектура за целите на кибернетичната отбрана, така че да се включат обхватът, функциите и изискванията, използвани в тази област от държавите членки на базата на националното законодателство и законодателството на ЕС.

Държавите членки на доброволна основа:

- ще подобряват сътрудничеството между между военните екипи за незабавно реагиране при компютърни инциденти (CERT) с цел по-добра превенция и справяне с инциденти.
- ще се възползват от ПСС за по-нататъшно засилване на сътрудничеството в областта на кибернетичната отбрана, включително нови проекти.
- ще използват Европейския фонд за отбрана за съвместно развиване на способности за кибернетична отбрана.
- ще разработят общо разбиране по отношение на прилагането на клаузата за взаимна помощ в кибернетичната област, като същевременно се запази гъвкавостта ѝ.
- ще разработят базови изисквания относно кибернетичната отбрана за информационната инфраструктура.
- доколкото подобряването на способностите за кибернетична отбрана зависи от експертния опит в областта на мрежовата и информационната сигурност за граждански цели, ще се възползват от експертната помощ на ENISA, на органите на държавите членки в рамките на групата за сътрудничество за МИС и на други възможни субекти на равнище ЕС с експертен опит по отношение на киберсигурността в гражданската сфера.

Държавите членки, ЕСВД/ВСЕС, ЕКСО и EDA:

- ще разгледат възможността за разработване на обучение по кибернетична отбрана с оглед на сертифицирането на бойните групи на ЕС.

Комисията в сътрудничество с държавите членки:

- ще вземе под внимание въпросите в областта на кибернетичната отбрана в работните програми на Европейската програма за промишлено развитие в областта на отбраната и Европейски фонд за отбрана.

2. Повишаване на защитата на комуникационните и информационните системи на ОПСО, използвани от структури на ЕС

Без да се засяга ролята на екипа за незабавно реагиране при компютърни инциденти за институциите, органите и агенциите на ЕС (CERT-EU) в качеството му на централната координационна структура на всички институции, органи и агенции на Съюза за реагиране при кибернетични инциденти и в рамките на съответните правила за бюджета на Съюза, ЕСВД ще развива адекватно и автономно разбиране за въпросите на сигурността и мрежовата защита и ще разработва собствен капацитет за сигурност на информационните технологии. Целта ще бъде да се подобри устойчивостта на управляваните от ЕСВД мрежи на ОПСО с акцент върху превенцията, откриването, реакцията при инциденти, ситуационната осведоменост, обмена на информация и механизмите за ранно предупреждение.

Генерална дирекцията „Бюджет и администрация“ (БА) на ЕСВД ръководи работата по защитата на комуникационните и информационните системи на ЕСВД и разработването на капацитет за сигурност на информационните технологии. Допълнителни специални ресурси и подкрепа ще бъдат предоставени и от Военния секретариат на Европейския съюз (ВСЕС), дирекцията за управление и планиране при кризи (CMPD) и способностите за планиране и провеждане на граждански операции (CPCC). Тази способност за сигурност на информационните технологии ще обхваща както класифицирани, така и некласифицирани системи и ще бъде неотменна част от съществуващите оперативни структури.

Необходимо е още оптимизиране на правилата за сигурност на информационните системи, предоставяни от различни институции на ЕС при провеждането на мисии и операции по линия на ОПСО. В този контекст, за да се подобри устойчивостта на мрежите, използвани за ОПСО, може да се помисли за единна верига на командване.

С цел по-добра координация и за повишаване на защитата и устойчивостта на комуникационните и информационните системи и мрежи на ОПСО, през 2017 г. в рамките на ЕСВД беше създаден вътрешен Управителен съвет по въпросите на киберсигурността под ръководството на генералния секретар на ЕСВД.

ЕСВД/БА:

- ще укрепва, въз основа на съществуващите технически способности и процедури, капацитета за сигурност на информационните технологии в ЕСВД с акцент върху превенцията, откриването, реакцията при инциденти, ситуационната осведоменост, обмена на информация и механизма за ранно предупреждение. Ще бъде доразвита стратегия за сътрудничество със CERT-EU и съществуващите способности на ЕС за кибернетична сигурност.

ЕСВД/БА заедно с ВСЕС, МРСС, CMPD и СРСС:

- ще разработват съгласувани политики и насоки за сигурност на информационните технологии, като вземат предвид и техническите изисквания за кибернетична отбрана на структури, мисии и операции в контекста на ОПСО, при отчитане на съществуващите рамки и политики за сътрудничество в ЕС, за да се постигне сближаване на правилата, политиките и организацията.

ЕСВД/единно звено за анализ на разузнавателна информация (SIAC):

- като се основава на съществуващите структури, ще подобрява оценката на кибернетичната заплаха и разузнавателните способности с цел определяне на нови кибернетични рискове и предоставяне на редовни оценки на риска, основани на стратегическата оценка на заплахата и информацията за инциденти в почти реално време, която се координира между съответните структури на ЕС и е достъпна на различни нива на класификация.

ЕСВД/SIAC и CERT-EU:

- ще насърчават обмена на информация за кибернетични заплахи в реално време между държавите членки и съответните образувания на ЕС. За тази цел между съответните национални и европейски органи ще се разработват механизми за споделяне на информация и мерки за изграждане на доверие въз основа на доброволен подход, който използва за отправна точка съществуващото сътрудничество.

ЕСВД/ВСЕС и МРСС:

- ще продължат да разработват и интегрират в стратегическото планиране концепция за кибернетична отбрана за военните мисии и операции по линия на ОПСО.
- ще разработят, в сътрудничество с оперативния щаб, обща оперативна стандартна процедура за кибернетичните аспекти на оперативно ниво.

ЕСВД/CPCC и CMPD:

- ще продължат да разработват и да интегрират в рамките на стратегическото планиране концепция за кибернетична отбрана за гражданските мисии по линия на ОПСО.
- ще укрепват способностите за кибернетична отбрана на гражданските мисии по линия на ОПСО, като се основават на съществуващата инфраструктура и насърчават стандартизацията и хармонизацията на технологиите, използвани в рамките на мисиите и операциите по линия на ОПСО, като се възползват, по целесъобразност, от експертния опит на CERT-EU, ENISA и EDA.
- в процеса на укрепване на гражданското измерение на ОПСО ще продължат да разглеждат възможностите за евентуална подкрепа на приемащите държави във връзка с кибернетичната сигурност чрез граждански мисии по линия на ОПСО.

ЕСВД:

- ще продължи да разработва общи изисквания за военните и гражданските мисии и операции по линия на ОПСО.
- ще засилва координацията в областта на кибернетичната отбрана с оглед на изпълнение на целите, свързани със защитата на мрежи, използвани от институции на ЕС в подкрепа на ОПСО, като за отправна точка се използва наличният в целия ЕС опит.
- въз основа на променящите се заплахи ще прави редовен преглед на изискванията за ресурсите и на съответните други решения, свързани с политиката, като се консултира с държавите членки и други институции на ЕС.

3. Насърчаване на гражданско-военното сътрудничество

Киберпространството е бързо развиващата се област: технологичните постижения трябва да бъдат укрепени чрез системи за сигурност както в гражданската, така и във военната сфера. Доколкото е възможно, следва да се предвиди координация между гражданската и военната сфера, когато сходни технологически постижения предоставят решения, приложими за гражданския и военния сектор. В други случаи военните способности и оръжейните системи са толкова специфични, че няма възможност за обмен с гражданските технологии. Без да се засягат вътрешната организация и националното законодателство на държавите членки, гражданско-военното сътрудничество в сферата на киберпространството може да се разглежда, наред с другото, с цел обмен на най-добри практики, обмен на информация и механизми за ранно предупреждение, оценки на риска във връзка с реагирането при инциденти и повишаване на осведомеността, както и провеждане на обучения и учения.

Повишаването на гражданската кибернетична сигурност е важен фактор, който допринася за цялостната устойчивост на мрежовата и информационната сигурност. Директивата за мрежова и информационна сигурност повишава готовността на национално равнище и укрепва сътрудничеството между държавите членки на равнището на Съюза както в стратегически, така и в оперативен план. Това сътрудничество включва както националните органи, осъществяващи надзор върху политиките в областта на кибернетичната сигурност, така и националните CERT и CERT-EU. Сътрудничеството между гражданските и военните CERT следва да се укрепва, като надлежно се отчита това развитие. Новият европейски Акт за киберсигурността има за цел да се повиши европейската устойчивост на кибератаки и да се осигури рамка за сертифициране на киберсигурността за продукти и услуги, като по този начин се увеличи доверието в гражданската цифрова сфера.

EDA, Агенцията на Европейския съюз за мрежова и информационна сигурност (ENISA), Европейският център за борба с киберпрестъпността (EC3) и CERT-EU, заедно с други имащи отношение органи и агенции на ЕС, в рамките на съответните им мандати и без припокриване с областите на компетентност на държавите членки, както и държавите членки, се насърчават да засилят сътрудничеството си в следните области:

- разработване на общи профили на компетентност в областта на кибернетичната сигурност и кибернетичната отбрана въз основа на най-добрите международни практики и сертифицирането, използвано от институциите, органите и агенциите на ЕС, като се вземат предвид и стандартите за сертифициране на частния сектор.
- принос за по-нататъшното разработване и адаптиране на организационните и техническите стандарти в областта на кибернетичната сигурност и кибернетичната отбрана, действащи в обществения сектор, с цел използването им в сектора на отбраната и сигурността. При необходимост за тази цел може да се използва текущата работа на ENISA и EDA.
- създаване или доразвиване на работни механизми и договорености за обмен на най-добри практики, по-специално във връзка с образованието, обучението и ученията, както и научните изследвания и технологиите и други области, даващи възможност за гражданско-военни полезни взаимодействия.
- използване на натрупания опит на ЕС, свързан със способностите за превенция и разследване на киберпрестъпността и свързаните с криминалистиката способности в тази област, както и по-широкото им използване за развиване на способности за кибернетична отбрана.

Държавите членки на доброволна основа:

- ще укрепват сътрудничеството между гражданските и военните CERT между държавите членки.

ЕСВД, Комисията и държавите членки:

- ще включват кибернетичната отбрана в процедурите на ЕС за управление на кризи и бедствия (чрез предвидения в плана процес).

4. Научни изследвания и технологии

Поради наличието на общи изисквания по отношение на технологиите и оперативния капацитет операторите на инфраструктура и доставчиците на ИКТ услуги за граждански и отбранителни цели са изправени пред сходни предизвикателства по отношение на кибернетичната сигурност. Общите потребности, свързани с научните изследвания и технологиите, и общите изисквания за системите се определят предварително, за да се подобри оперативната съвместимост на системите в дългосрочен план и да се намалят разходите за намиране на решения. Постигането на икономии от мащаба е необходимо, за да се отговори на все по-големия брой заплахи и уязвими точки. Това от своя страна следва да спомогне за запазването и развитието на конкурентоспособността на сектора на кибернетичната отбрана в Европа.

Научните изследвания и технологиите са важни за развитието на способностите за кибернетична отбрана. В рамките на програмата за научни изследвания в областта на кибернетичната отбрана EDA е предоставила солидна основа за определяне на приоритетите на бъдещото финансиране в областта на научните изследвания и технологиите в междуправителствената рамка. Последващата стратегическа научноизследователска програма, разработена в рамките на съответната *ad hoc* работна група на EDA, осигурява информирано определяне на приоритетите във връзка с кибертехнологиите, необходими във военната област, като в същото време установява възможности за усилия и инвестиции с двойна употреба, независимо дали в национални или многонационални условия или чрез финансиране от ЕС.

От съществено значение е създаването на технологичен капацитет в Европа с цел намаляване на заплахите и уязвимостта. Промишлеността ще остане основен двигател по отношение на свързаните с кибернетичната отбрана технологии и иновации. Сред областите, на които трябва да се обърне внимание, са криптографията, сигурните вградени системи, откриването на зловреден софтуер, техниките за симулация и визуализиране, защитата на мрежовите и комуникационните системи и технологиите за идентификация и установяване на автентичността. Освен това е важно да се поощрява изграждането в Европа на конкурентоспособна промишлена верига на доставките в областта на кибернетичната сигурност чрез подкрепа на участието на малките и средните предприятия (МСП).

Целта да се гарантира, че Европа може да бъде в крак с международните конкуренти по отношение на технологичните способности в кибернетичната област, зависи и от нашата способност за стимулиране на авангардни нововъведения чрез национални инструменти и инструменти на ЕС, например Европейския съвет по иновациите.

За да се улесни гражданско-военното сътрудничество в областта на развитието на способности за кибернетична отбрана, да се укрепи европейската отбранителна технологична и индустриална база[10] и да се допринесе за стратегическата автономност на ЕС и в областта на киберпространството, когато и където е необходимо и при възможност съвместно с партньори**,**

EDA, Комисията и държавите членки:

- ще търсят взаимодействия между научните изследвания и технологиите във военния сектор и гражданските програми за научноизследователска и развойна дейност, по-специално по отношение на авангардните нововъведения, и ще вземат под внимание измерението на кибернетичната сигурност и кибернетичната отбрана при осъществяването на подготвителното действие за научни изследвания в областта на отбраната.
- ще обменят научноизследователски програми в областта на кибернетичната сигурност (напр. стратегическата научноизследователска програма на Европейската агенция по отбрана в областта на кибернетичната сигурност), както и произтичащите от тях пътни карти и действия; за тази цел ще бъде изготвена междусекторна програма за научни изследвания в областта на кибернетичната отбрана в тясно сътрудничество с Комисията и държавите членки.
- ще съдействат за по-пълното интегриране на кибернетичната сигурност и кибернетичната отбрана в програмите, които включват аспекти на сигурността и отбранителните технологии с двойно предназначение, например Програмата за изследване на управлението на въздушното движение в единното европейско небе (SESAR).

[10] Съобщение на Комисията „За по-конкурентоспособен и по-ефективен сектор на отбраната и сигурността“, COM (2013) 542

Комисията:

- ще обмисли създаването на Европейски център за промишлени, технологични и изследователски експертни познания в областта на киберсигурността с Мрежа от национални координационни центрове с цел подпомагане на технологичния и промишления капацитет в областта на кибернетичната сигурност и повишаване на конкурентоспособността на сектора на кибернетичната сигурност на Съюза, като се гарантира взаимно допълване и се избягва дублирането в рамките на Мрежата от центрове за компетентност по киберсигурността и други агенции на ЕС. Центърът следва, наред с другото, да засили сътрудничеството между гражданските и отбранителните технологии и приложения, като работи тясно и при пълно взаимно допълване с Европейската агенция по отбрана в областта на кибернетичната отбрана.
- ще оказва подкрепа за развитието на промишлени екосистеми и иновационни клъстери по цялата верига на създаване на стойност в областта на сигурността, като за целта се опират на академичните знания, иновациите на МСП и промишленото производство.

Комисията, в сътрудничество с държавите членки:

- ще вземе под внимание въпросите в областта на кибернетичната отбрана в поканите за отправяне на предложения на подготвителното действие за научни изследвания в областта на отбраната.
- ще разгледа кибернетичната отбрана сред темите, повдигнати за разглеждане от Европейския фонд за отбрана.
- ще подкрепи съгласуването на политиката на ЕС, за да се гарантира, че политическите и техническите аспекти на кибернетичната защита в ЕС ще останат в челните редици на технологичните иновации, както и че те са хармонизирани в рамките на целия ЕС (способности за анализ и оценка на кибернетичните заплахи, инициативи за сигурност при проектирането, управление на зависимостите при достъпа до технологии и т.н.).

5. Подобряване на възможностите за образование, обучение и учения

За да се увеличи готовността за справяне с киберзаплахи и да се развие обща култура на кибернетичната отбрана в целия ЕС, която да е от полза и за мисиите и операциите на ЕС, е необходимо да се подобрят и увеличат възможностите за обучение в областта на кибернетичната отбрана. От решаващо значение е бюджетите за образование и обучение да се използват ефективно, като същевременно се осигурява възможно най-добро качество. Обединяването и споделянето на европейско равнище в областта на образованието и обучението, свързани с кибернетичната отбрана, ще бъдат от решаващо значение.

Европейският колеж по сигурност и отбрана (ЕКСО), ЕСВД, EDA, Комисията и държавите членки:

- въз основа на анализа на EDA на нуждите от обучение по кибернетична отбрана и на натрупания от ЕКСО опит в обучението по кибернетична сигурност ще се създадат възможности за обучение и образование по линия на ОПСО за различна аудитория, в т.ч. ЕСВД, личен състав на мисиите и операциите по линия на ОПСО и длъжностни лица от държавите членки, чрез което следва да се намери решение и на въпросите, свързани със задържането на квалифициран персонал в краткосрочен, средносрочен и дългосрочен план.
- ще предложат да бъде установен диалог с държавите членки, институциите на ЕС, трети държави и други международни организации, както и с частния сектор, по въпросите на стандартите в обучението и сертифицирането в сферата на кибернетичната отбрана.
- ще установят сътрудничество с европейски доставчици на услуги за обучение от частния сектор, както и с академични институции, с цел повишаване на компетентността и уменията на личния състав на мисиите и операциите по линия на ОПСО.

ЕКСО:

- ще продължи да разработва платформата за образование, обучение, оценка и учения в кибернетичната област, установена в рамките на ЕКСО (киберплатформата ETEE).
- ще изгражда взаимодействия с програмите за обучение на други заинтересовани страни, например ENISA, Европол, Европейския полицейски колеж (CEPOL) и Съвместния център на НАТО за високи постижения в областта на кибернетичната отбрана.
- ще проучва възможностите за съвместни програми за обучение на ЕКСО и НАТО в сферата на кибернетичната отбрана, които ще бъдат отворени за всички държави — членки на ЕС, с цел да се насърчи обща култура в областта на кибернетичната отбрана.

Комисията:

- ще оценява вариантите за увеличаване на възможностите за образование и обучение в държавите членки, установени от киберплатформата ETEE.

EDA:

- ще разработва още курсове в сътрудничество с ЕКСО, за да се отговори на изискванията на държавите членки по отношение на образованието, обучението и ученията в областта на кибернетичната отбрана.
- ще подпомага киберплатформата ETEE, наред с другото, чрез постепенно включване на модули за образование, обучение, оценка и учения в кибернетичната област, разработени в рамките на EDA.

ЕСВД и държавите членки:

- в тясно сътрудничество със съответните служби на институциите, органите и агенциите на ЕС и въз основа на съществуващите стандарти и знания, ще следват установените механизми на ЕКСО за сертифициране на програмите за обучение. ще разгледат възможността за създаване на специфични за кибернетичното пространство модули в рамките на военната инициатива „Еразъм“.

Необходимо е да се подобрят възможностите за учения в областта на кибернетичната отбрана за военните и гражданските участници в рамките на ОПСО. Съвместните учения са инструмент за разработване на общи познания и разбиране за кибернетичната отбрана. Това ще даде възможност на националните сили да подобрят своята готовност да работят в многонационална среда. Провеждането на съвместни учения в областта на кибернетичната отбрана ще допринесе и за изграждането на оперативна съвместимост и доверие.

ЕСВД, EDA, CERT-EU и държавите членки ще поставят акцент върху насърчаването на елементите на кибернетичната отбрана в ученията на ОПСО и други учения:

- интегриране на измерението на кибернетичната отбрана в съществуващите сценарии за учения за *MILEX* и *MULTILAYER*.
- редовно организиране на стратегически/политически учения като *CYBRID 2017* в координация с воденото от ЕС паралелно и координирано учение (PACE) и оперативно-технически учения като *DEFNET*.
- разработване, по целесъобразност, на специализирано учение в областта на кибернетичната отбрана на ЕС по линия на ОПСО и разглеждане на възможностите за координация с общоевропейски кибернетични учения, например *CyberEurope*, организирано от ENISA.
- продължаване на участието в други многонационални учения в областта на кибернетичната отбрана, например *Locked Shields*.
- отправяне на покани към съответните международни партньори, например НАТО, да участват в ученията, в съответствие с рамката на политиката на ЕС за ученията.
- организиране на редовни учения въз основа на инструментариума за кибердипломация, в рамките на които държавите — членки на ЕС, могат да се упражняват в реагиране на злонамерени действия в киберпространството.

6. Засилено сътрудничество с подходящи международни партньори

В рамките на международното сътрудничество е необходимо да се осигури диалог с международните партньори, по-специално НАТО и други международни организации, което да допринесе за развитието на ефективни способности за кибернетична отбрана. Следва да търси по-голяма ангажираност с работата, извършвана в рамките на Организацията за сигурност и сътрудничество в Европа (ОССЕ) и Организацията на обединените нации (ООН), с оглед да се представи стратегическа рамка за предотвратяване на конфликти, сътрудничество и стабилност в киберпространството.

В ЕС е налице политическа воля за продължаване на сътрудничеството с НАТО в областта на кибернетичната отбрана за развиване на стабилни и устойчиви способности за кибернетична отбрана според изискванията, определени в съвместната декларация, подписана от председателя на Европейския съвет, председателя на Европейската комисия и генералния секретар на Организацията на Северноатлантическия договор във Варшава на 8 юли 2016 г. Провеждането на редовни консултации между службите на тези организации, на междуинституционални брифинги, както и на евентуални общи заседания на Политико-военната група и съответните комитети на НАТО, ще спомогне за избягване на ненужното дублиране на работата и осигуряване на последователност и взаимно допълване на усилията в съответствие с посочената по-горе рамка.

ЕСВД и EDA, съвместно с държавите членки, ще доразвиват сътрудничеството между ЕС и НАТО в сферата на кибернетичната отбрана, при надлежно зачитане на институционалната рамка и автономността на тези организации при вземането на решения, посредством:

- активизиране на текущите дейности в рамките на изпълнението на съвместната декларация на председателя на Европейския съвет, председателя на Европейската комисия и генералния секретар на Организацията на Северноатлантическия договор.
- обмен на най-добри практики при управлението на кризи, както и по отношение на кибернетичната отбрана в рамките на военните и гражданските мисии и операции.
- осигуряване на единност на резултатите при разработването на изискванията за способностите за кибернетична отбрана, когато те се припокриват, и по-специално при развитието на капацитета за кибернетична отбрана в дългосрочен план.
- по-активно използване на рамката на EDA за сътрудничество със Съвместния център на НАТО за високи постижения в областта на кибернетичната отбрана като първоначален форум за засилено сътрудничество по многонационални проекти, свързани с кибернетичната отбрана, въз основа на подходящи оценки.

ЕКСО, ЕСВД и EDA:

- ще засилят сътрудничеството, свързано с концепциите за обучение, образование и учения в областта на кибернетичната отбрана.
- ще гарантират реципрочно участие на персонала в ученията в съответствие с договорената рамка.

CERT-EU:

- ще продължи да използва техническото споразумение между CERT-EU и NCIRC (екипа на НАТО за реагиране при компютърни инциденти) с цел подобряване на ситуационната осведоменост, обмена на информация и механизмите за ранно предупреждение и прогнозиране на заплахи, които биха могли да засегнат и двете организации.

По отношение на други международни организации и съответните международни партньори на ЕС, по целесъобразност ЕСВД и държавите членки:

- ще следят стратегическите развития и ще провеждат консултации по въпросите на кибернетичната отбрана с международните партньори (международни организации и трети държави).
- ще проучват възможностите за сътрудничество в областта на кибернетичната отбрана, в т.ч. с трети държави, участващи в мисии и операции по линия на ОПСО.
- ще насърчават в рамките на съответните международни организации, по-специално ООН, ОССЕ и Регионалния форум на АСЕАН, прилагането на съществуващото международно право, по-специално Устава на ООН в неговата цялост, в областта на киберпространството, изготвянето и прилагането на универсални необвързващи норми на отговорно поведение на държавите и регионални мерки за изграждане на доверие (МИД) между държавите с цел повишаване на прозрачността и намаляване на риска от погрешно възприемане на поведението на дадена държава.

Комисията и ЕСВД:

- по целесъобразност ще подпомагат изграждането на киберспособности за партньорите на ЕС чрез изменения инструмент, допринасящ за стабилността и мира.

Последващи действия

След координация от страна на ЕСВД на изпълнението на ПРКО ЕСВД/ EDA/ Комисията следва да представят годишен доклад за напредъка, който да включва шестте очертани по-горе области, на Политико-военната група, с участието на членовете на Хоризонталната работна група по въпроси на кибернетичното пространство, и на Комитета по политика и сигурност с цел оценка на изпълнението на ПРКО. На всеки шест месеца ще има и устно представяне.

С нарастването на кибернетичните заплахи е особено важно да се набелязват нови изисквания относно кибернетичната отбрана, които впоследствие да бъдат включени в рамката за политиката на ЕС за кибернетична отбрана. Следващото преразгледане на ПРКО следва да бъде представено не по-късно от средата на 2022 г., след тесни консултации с държавите членки.